Google Cloud

Perspectives on Security for the Board

October 2023 – Edition 3

Office of the CISO

October 2023

Table of contents

Foreword

Boards can focus on security by, oddly enough, not just focusing on security. What this means is focusing on whether your organization is investing enough in modernizing technology. One of the things that happens when boards just focus on cybersecurity as a siloed priority is you tend to get a disproportionate amount of investment in cyber, and less on upgrading what may be older legacy systems and architectures.

We must get to a point where every organization is prioritizing using a technology platform where security is built in, and not bolted on after the fact. That requires management, especially the CIO, the CTO, and the CISO to really partner on driving their technology platform to be in a more defendable state.

Boards can help with that by asking the right questions of management to make sure that they're investing in technology broadly. The benefits aren't just limited to security. If you have a more modern digital infrastructure to support your business that's been built with security in mind, you are going to get better security outcomes – but you're also going to get more efficiency, reliability, and agility in deploying and building new products and new features. The engagement of the board more deeply on the strategic positioning of technology, not just on security, brings a larger set of positive outcomes for the organization.

Boards should help guide management to invest strategically in new business initiatives. And, when these investments are made, boards should help execute those new initiatives by ensuring security is baked in – and not in a way where security teams are having to play catch-up.

To help boards understand how better to engage with their security leaders, this edition of our Perspectives on Security for the Board report covers: 1) threat activity reported on in Q3 2023, and how boards can support their organizations defend against it, 2) the ins and outs of effective crisis communications, and how boards can work with leaders across the organization to be ready to respond to a cyber incident, 3) AI and red teaming, and how boards can help ensure AI investments are secure.

We hope you find this report informative, and we look forward to connecting with you more on these important topics

Phil Venables (CISO, Google Cloud)

Navigating the Global Threat Landscape — Initial Infection Vector Is Where It All Begins

Breaches typically involve many steps and components, but they all start somewhere. In cybersecurity, we refer to that as the initial infection vector. The attacker will use a technique or multiple techniques to gain access to a network, and from there perform actions such as moving laterally and escalating privileges to achieve their objectives. These objectives could be anything from obtaining customer information for extortion purposes, to stealing trade secrets such as confidential research and development.

For victim organizations, this can lead to significant financial, reputational, and other damages. Board members who understand cyber threats are in a strong position to help ensure their organizations are protected against attacks, and also can help lead their organizations to positive outcomes when the attackers are successful.

Initial infection vector research released in Q3 2023

There are few threats, if any, that are more well-known than phishing. Common scams involve imitating well-known brands and requesting personal information such as credentials and payment information, but phishing can be much more sophisticated and challenging to detect. In fact, it is one of the most common ways that attackers get into organizations. Of all the investigations covered in our M-Trends 2023 report, phishing was the second most utilized initial infection vector globally at 22% (exploits were number one at 33%), and number one in the EMEA region at 40%. When phishing attempts against employees are successful, the impact to business can be significant. Attackers can use even the lowest level access to ultimately achieve their goals.

Here are examples of phishing activity our cybersecurity researchers, analysts and consultants examined in recent months:

- **What happened?** A Russian espionage group has increased the tempo and frequency of their phishing operations in the first half of 2023, since Ukraine launched its counteroffensive. These diplomatic-themed phishing campaigns targeted a wide range of diplomatic representations in Kyiv, including those of Moscow's partners, and likely reflect a growing mission to obtain political intelligence. These operations demonstrate steps attackers take to evade detection, including incorporation of anti-analysis components.
  - » **For your CISO**: Read our research on these phishing espionage operations.

(Navigating the Global Threat Landscape — Initial Infection Vector Is Where It All Begins, cont'd.)

- **What happened?** A financially motivated group has persistently used phone-based social engineering and SMS phishing campaigns (smishing) to obtain credentials to gain and escalate access to victim organizations. The group directs victims to convincing phishing login pages, and also has contacted help desks to perform password resets. The group has been observed deploying ransomware and stealing large amounts of data for extortion purposes.
  - » **For your CISO**: Read our research on these smishing cyber crime operations.

Another initial infection vector that is growing in popularity is infected USB drives. These devices are prevalent across all organizations, and are commonly given away as swag at conferences and events. In the first half of 2023, Mandiant Managed Defense observed a threefold increase in the number of attacks using infected USB drives to steal secrets. Here are two of these recent campaigns:

- **What happened?** A China-linked espionage group was observed leveraging infected USB flash drives to distribute a backdoor (malware used to bypass normal authentication). The backdoor was used to collect information in support of Chinese national security and economic interests. These operations pose a risk to a variety of industries — including construction and engineering, business services, government, health, transportation, and retail — in Europe, Asia, and the United States.
- **What happened?** An attacker was observed leveraging infected USB flash drives to distribute malware that creates a backdoor on the host system, giving attackers the ability to remotely issue system commands. It also spreads to other USB flash drives and propagates throughout the network. We attribute this campaign to a group that has targeted oil and gas organizations in Asia.
  - » **For your CISO**: Read our infected USB drive research.

Over the summer we saw a high volume of zero-day vulnerability abuse by malicious actors with various motivations, which we covered in greater detail in our previous report. We consider a zero-day to be a vulnerability that was exploited in the wild before a patch was made publicly available. The zero-day vulnerabilities we reported on in the previous report impacted big tech companies, including Barracuda and VMware. While the volume of zero-day related attacks has tapered off, we are still seeing activity:

- **What happened?** On July 18, Citrix announced vulnerabilities in Netscaler ADC and Netscaler Gateway (network appliances), one of which could be exploited to perform arbitrary code execution. Arbitrary code execution enables attackers to run any command or code on a system, making it one of the most severe threats. Based on our investigations and research, we believe a likely China-nexus attacker was exploiting the vulnerability for espionage purposes.
  - » **For your CISO**: Read our Citrix zero-day research, and utilize our Indicators of Compromise scanner.

(Navigating the Global Threat Landscape — Initial Infection Vector Is Where It All Begins, cont'd.)

Putting this in action

Understanding the breadth, pace, and diversity of the threat landscape is pivotal if you want to help your organization stay ahead of and respond to them. Boards can help ensure their organizations are prepared for and protected against attacks that begin with phishing, smishing, infected USB drives, and zero-day vulnerabilities by sharing the research and guidance we provided with their CISOs and security teams. Boards can — and should — also participate in broader security conversations on these topics.

Ask your CIO/CTO and CISO:

- What is our strategy to deploy tokens or other forms of authentication to reduce a wider array of risks?
- Can our approach to authentication be by-passed and how are we monitoring that risk?
- How are we keeping our systems up to date against the latest threats?
- What are we doing to appropriately prioritize, track and patch the most critical vulnerabilities in our network?
- Are any necessary security enhancements being held back by operational, commercial or budget constraints?
- Are security measures interfering with usability and needed business agility and what are the CIO and CISO doing to resolve that so we're getting good security outcomes without having to compromise customer support?

Cybersecurity is challenging for even the most security-mature organizations, and sometimes it helps to have the right external partnerships to complement your internal relationships. Boards should work with their business, IT and security (CISO) leadership to bring external cybersecurity partners such as Google to the table to help reduce the risk posed by these types of cyber threats, and translate frontline intelligence into actionable information.

Board Ready for Crisis Communications Response in the Digital Age

In today's rapidly evolving digital landscape, the intersection of cybersecurity and crisis communications has never been more critical. As we continue to witness an unprecedented surge in cyber threats and incidents, the ability to effectively oversee cyber risk – including preparedness and response to these crises – becomes paramount.

In this section, we explore the latest trends and strategies that empower defenders to safeguard digital assets while maintaining open lines of communication during times of crisis. While the board may not necessarily have a direct communications role, they will likely serve in an advisory and oversight capacity in preparing for and responding to incidents, making this a critical topic to be aware of.

Current environment

A well-defined incident response and crisis communication plan is essential for minimizing the impact of a cyber incident. Timely detection, containment, eradication, and recovery are key stages in this process, coupled with a sound strategy for communications and stakeholder engagement. Meanwhile, effective crisis communications is also integral to maintaining trust and transparency with stakeholders. In today's interconnected world, a swift and coordinated response is imperative. Social media platforms, official statements, and regular updates via multiple channels are all crucial components of a successful crisis communications strategy.

What leads to the best crisis communications response?

With specific attention to crisis communications, we will share lessons learned from Mandiant's Crisis Communications response specialists' first-hand experience addressing cybersecurity crisis communications planning during four phases: strategic readiness, assurance, response, and post-incident review.

Phase 1: Strategic readiness

First in the cycle is the pre-breach "Strategic Readiness" phase or simply stated, the planning phase. This phase is a foundational and essential activity for all organizations, regardless of size, sector, or location. The approach should be customized to the organization, providing a written and repeatable plan with clearly defined roles and responsibilities, a governance structure with formal decision authority levels, and a framework for response. This team should include representation from across the organization (including HR, Procurement, Communications, Legal, Logistics, and Operations to name a few). You can't anticipate what you'll need, especially when it comes

(Board Ready for Crisis Communications Response in the Digital Age, cont'd.)

to provisioning hardware, disseminating actionable intelligence, and conducting insightful data impact assessments. The team should also implement a governance and management model, with specific working groups aligned to functional responsibilities.

One of the deliverables developed during the planning phase is a Crisis Communications annex to the Incident Response Playbook. This playbook should be specific to the organization and include sections on incident and crisis response, key messaging based on hypothetical scenarios, and stakeholder identification and channel mapping. One additional consideration is the importance of having alternative communication mechanisms, commonly referred to as "out of band" communications, in the event your primary way of communication is compromised. In data breach and cybersecurity incidents, an attacker may still have access to the network (known as persistence), requiring leaders and responders to use these alternative communication methods.

Staying compliant with evolving cybersecurity regulations and data privacy standards is non-negotiable. This ensures that we not only meet legal and regulatory requirements, but also maintain the trust and confidence of stakeholders. Globally, governments are enacting more regulations requiring greater transparency and personal accountability for incidents. As an example, the U.S. Securities & Exchange Commission recently issued new Cybersecurity Disclosure Regulations. For more details on the regulation, check out this article on 7 Essential Steps to Prepare Your Whole Organization for a Cyber Incident.

Phase 2: Assurance

The second phase, also part of the proactive and pre-breach response, is the "Assurance" or exercise phase. During this phase, companies should exercise their team's response based on real-world attacks and scenarios. Some states are even moving to mandate this as part of the board response. Regularly conducting cybersecurity tabletop exercises and crisis simulations can significantly enhance your preparedness. These exercises not only help refine incident response processes, but also provide invaluable experience for organizations in managing real-world scenarios.

Phase 3: Incident Response

The third phase is the reactive phase of "Incident Response." Response execution will be defined by the priority and attention you put into the first two phases. When the day comes, it is imperative that organizations are able to quickly spin up their teams for response. They will know their roles and responsibilities, and have a working governance structure to respond. They will be able to organize the requisite information exchange sessions, and track the action items and tasks. They will have already mapped their stakeholders and communication channels, and be able to quickly assess channel readiness. The smoothest and most-effective responders are usually those who are well-trained, well-equipped, and have pre-staged the requisite tools ahead of time.

[1] *New York State Department of Financial Services, DFS Superintendent Adrienne A. Harris Announces Updated Cybersecurity Regulation, November 2022*

(Board Ready for Crisis Communications Response in the Digital Age, cont'd.)

Phase 4: Post-incident review

Managing a breach is hard, both from an emotional and an operational standpoint, and many people never want to talk about the incident again. However, as difficult as it may be, it's important to move to the final phase: the Post-Mortem Assessment. This phase starts just as the dust settles — the investigation is complete, the remediation activities restored business operations, and notifications have been made to regulators or victims. Some may also call this the "After Action" or "Lessons Learned" phase, and second to planning, it is one of the most important phases.

To hear more frontline stories on how Mandiant Crisis Communications supports breaches through these phases, check out this podcast.

Putting this in action

The dynamic nature of cybersecurity threats calls for a board-led multifaceted approach combining robust technical defenses and effective crisis communications strategies. By integrating these programs into your cybersecurity and crisis management framework, you'll be better equipped to safeguard your organization's digital assets and reputation.

As board members, it is important to understand your role related to incident response and operational readiness.

Ask your C-suite, IT and security (CISO) leadership:

- What is your role in the event of a cyber incident?
- Do you know your organization's regulatory and legal reporting requirements when it comes to an information security, data, or privacy incident?
- Do you know how you will be contacted in the event of an incident and have a process in place to authenticate the communications?
- Do you have a secure way to share and receive communications related to an incident?
- Are you receiving regular threat intelligence briefs that will help inform your risk-based decision making?
- Have you confirmed your organization has cyber incident response plans, playbooks and documentation?
- Do you know your organization's ransom payment strategy?
- Are you participating in executive tabletop exercises?

AI and Red Teaming

In the last report, we introduced the Secure AI Framework (SAIF), a conceptual framework for secure AI systems that boards can use to help ensure their organizations utilize AI in a responsible way. In this report, we'll explore one critical capability that we deploy to support SAIF: red teaming.

Red teaming is one way that organizations can help adjust mitigations and create faster feedback loops for AI deployment (element five of SAIF). More broadly, we believe that red teaming will play a decisive role in preparing every organization for attacks on AI systems, and recommend boards work with the CISO to explore the following three areas to help assess whether and how to stand up a dedicated AI Red Team.

First, boards should understand what red teaming in the context of AI systems is and why it is important. Whether organizations ultimately choose to deploy red team capabilities depends on the AI use case, and the board should work with the CISO to ensure the implementation of the SAIF (including red teaming) captures the complexities and risks of the particular deployment. A Red Team consists of a team of hackers that simulate a variety of adversaries, ranging from nation states and well-known Advanced Persistent Threat groups to hacktivists, individual criminals or even malicious insiders. Over the past decade, Google has evolved our approach to translate the concept of red teaming to the latest innovations in technology, including AI. The AI Red Team is closely aligned with traditional red teams, but also has the necessary AI subject matter expertise to carry out complex technical attacks on AI systems. This alignment is important to ensure that they are simulating realistic adversary activities.

Putting this in action

- Partner with CISO to understand more about how red teams operate and whether your organization can better leverage red teams to improve defenses, and determine whether additional investment is needed.

Second, boards should work with the CISO to understand how your organization plans to take the latest threat intelligence and relevant research, and adapt it to work against real products and features that use AI to learn about their impact. Exercises can raise findings across security, privacy, and abuse disciplines, depending on where and how the technology is deployed. To identify these opportunities to improve safety, boards can work with the CISO to understand how they leverage attackers' tactics, techniques and procedures (TTPs) to test a range of system defenses. Boards can review our most recent red team report to learn more about common TTPs, including prompt attacks, training data extraction, backdooring the model, adversarial examples, data poisoning and exfiltration.

Putting this in action

- Request an annual briefing on TTPs that your CISO considers most relevant and realistic for real world adversaries and AI red teaming exercises, and how your defenses protect against them.

(AI and Red Teaming, cont'd.)

Finally, boards should work with the CISO to incorporate key lessons from red team exercises. We've already seen early indications that investments in AI expertise and capabilities in adversarial simulations are highly successful. Red team engagements, for example, have highlighted potential vulnerabilities and weaknesses, which helped anticipate some of the attacks we now see on AI systems.

Putting this in action

- Partner with the CISO to incorporate both security and AI subject matter experts for realistic end-to-end adversarial simulations.
- Partner with the CISO to create a feedback loop that ingests key learnings from red teams and quickly incorporates them into your system's protections.
- Request an annual briefing on your organization's plans to incorporate red teaming findings into research and product development efforts.

As with all red teaming efforts, boards should work closely with the CISO to continue to learn and develop new adversarial simulation techniques over time and as a result, improve defenses. Boards should consider red teams as a useful tool for taking SAIF one step further and getting educated, being engaged, and staying informed on AI and cybersecurity issues.

We'll continue to explore these topics in more detail in future reports. Read our paper for more information on Google's AI Red Team.

Conclusion

A constantly evolving threat landscape that can massively impact business; crisis communications plans to help organizations during incidents; securing AI tools and systems in a time of rapid innovation. All of the above underline why it's more important than ever for boards to partner with their organization's security leaders, and even enlist the help of external security experts, to stay current with the latest trends.

Our Perspectives on Security for the Board series is another way boards can be ready. Each report is written with the three principles for effective risk oversight in mind: 1) get educated; 2) be engaged; and 3) stay informed. This approach — along with strong relationships with security, technology and other related stakeholders — will help boards guide their organizations to positive security outcomes.

At Google Cloud, we look forward to working with you towards that goal. Head over to our Board of Directors Insights Hub for more actionable cybersecurity resources.

Google Cloud